Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
628 East 9th Street
Houston TX 77007-1722
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson
fjohnson@azalaw.com (SBN 289055)
AHMAD, ZAVITSANOS, & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston TX 77010
Tel: (713) 655-1101
Fax: (713) 655-0062

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

JANE DOE, individually and on behalf of others similarly situated,

Plaintiff,

v.

THE COUNTY OF SANTA CLARA d/b/a SANTA CLARA VALLEY MEDICAL CENTER

Defendant.

CASE NO. 3:23-cv-04411-WHO

PLAINTIFF'S RESPONSE TO DEFENDANT COUNTY OF SANTA CLARA'S MOTION TO DISMISS

Date: October 30, 2024
Time: 2:00 pm
Crtrm: 2, 17th Floor
Judge: Hon. William H. Orrick

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

I. INTRODUCTION

For the first time, after having litigated this case for over a year, Defendant Santa Clara County d/b/a Santa Clara Valley Medical Center ("Santa Clara") argues that this Court does not have jurisdiction under the Class Action Fairness Act ("CAFA"). Santa Clara, however, has not met its burden to prove that this Court should abstain from CAFA jurisdiction, and in any case has waived any objection to CAFA jurisdiction by asking this Court for affirmative relief on its first motion to dismiss, engaging in discovery, and only changing its mind regarding its preferred forum after the Court denied Santa Clara's first attempt to get the case dismissed. *See* Dkt. 64. In any case, federal question jurisdiction makes the CAFA issue immaterial. Because Plaintiff has pled a claim under the federal Electronic Communications Privacy Act ("ECPA"), jurisdiction also exists under 28 U.S.C. § 1331.

Santa Clara also renews its argument that it is immune, as a government entity, from all causes of action except Plaintiff's claims under California's Confidentiality of Medical Information Act ("CMIA")—the one cause of action that Santa Clara has never challenged. Regarding Plaintiff's ECPA claim, Santa Clara asks this Court to ignore Congress's explicit provision of a cause of action against government entities in 18 U.S.C. §§ 2520 (a) & (g) and instead follow a minority of courts who have considered the issue. Santa Clara's reading of the ECPA, however, would essentially nullify the Federal Wiretap Act's protections for citizens against government disclosures of illegally obtained information. This Court should reject it and instead follow the majority view of courts, including of the Sixth and Second Circuits, which holds that government entities are subject to federal wiretap statutes.

Furthermore, even if Plaintiff had not stated a claim for willful disclosure of improperly intercepted information under 18 U.S.C. §§ 2520 (a) & (g), Plaintiff also alleges that Santa Clara violated a separate provision of the ECPA, 18 U.S.C. § 2511(3)(a). This section prohibits any "person or entity" that provides an "electronic communications service" from intentionally disclosing the contents of a communication. 18 U.S.C. § 2511(3)(a). Even Santa Clara admits that this Section "creates a substantive right against a government entity." Mot. 11. Plaintiff's

Fourth Amended Complaint ("FAC") alleges that Santa Clara's patient portal provides an electronic communications service to patients, allowing them to message their doctors, view lab results, and refill prescriptions. FAC ¶ 20. Plaintiff further alleges that tracking pixels on the web version of Santa Clara's patient portal as well as Google Firebase code on Santa Clara's patient portal mobile app disclosed these communications to third parties. FAC ¶¶ 32-35. These allegations provide an independent ground for Plaintiff's ECPA claim and are in themselves sufficient to sustain both Plaintiff's federal wiretap cause of action and federal question jurisdiction.

Finally, because Plaintiff has alleged that Santa Clara violated "mandatory duties" under HIPAA and its state-law analog, the CMIA, as well as under the ECPA, Plaintiff has stated a claim under California Government Code Section 815.6.[1] Because these statutes provide important privacy protections to all patients—whether of a privately owned or public hospital—the Court should deny Santa Clara's Motion to Dismiss.

II. STANDARD OF REVIEW

At the pleading stage, the plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007). A claim is facially plausible when the plaintiff pleads facts that "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). In deciding whether a claim has been stated upon which relief can be granted, the court accepts all factual allegations as true and draws all reasonable inferences in favor of the plaintiff. *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). If a court dismisses any claim, leave to amend should be granted "unless it determines that the pleading

[1] Plaintiff does not contest Santa Clara's Motion to Dismiss her claims under CDAFA, CAL. PENAL CODE § 502, or CAL. CIVIL CODE § 1798.82. In addition, Plaintiff will not oppose the County's motion as it relates to punitive damages, but will continue to pursue actual damages, nominal damages, and statutory damages.

could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000).

III. FACTUAL AND PROCEDURAL BACKGROUND

Santa Clara operates a website and patient portal for patients where they can schedule medical appointments, review treatment information and test results, refill prescriptions, and communicate with doctors. (FAC ¶ 17.) Santa Clara's patient portal is available either via a web-based interface or via a mobile app. (*Id.* ¶ 34.) The Plaintiff Jane Doe is a Santa Clara Valley Medical Center patient who has regularly used Defendant's website and patient portal since 2018 to search for treatments for her conditions, including cirrhosis of liver and ascites, generalized anxiety disorder, migraines, and carpal tunnel syndrome. (*Id.* ¶ 19.) During these interactions with Defendant's website and patient portal, Plaintiff Jane Doe disclosed sensitive medical information about herself, including her patient status and medical conditions. (*Id.*)

Defendant knew the sensitivity of the health information that its patients disclosed through its website and patient portal, yet made the decision to integrate technologies—including the Meta Pixel and the Google Analytics pixel—on its website, including the navigation buttons to its patient portal. (*Id.* ¶¶ 26–31.) It also used Google Firebase code to serve the same function on its patient portal mobile app. (*Id.* ¶ 35.) These tracking technologies worked like a listening device. Each time Plaintiff Jane Doe typed a search term, the pixels recorded the information she entered and transmitted it to Facebook and Google, along with identifying information that let Facebook and Google know exactly who Jane Doe was. (*Id.* ¶¶ 32–33.) Instantaneously, Facebook and Google knew the conditions for which Plaintiff was seeking medical treatment. (*Id.*) This information then became available for advertisers to use when Facebook and Google sold them targeted advertising services. (*Id.* ¶ 36.)

After using Defendant's patient portal and website, Plaintiff saw numerous advertisements in her Facebook feed for products and services related to the medical conditions for which she had entered data inside the patient portal, including advertisements for pain management. (*Id.* ¶ 37.) These advertisements included advertisements for medications for her

various conditions, as well as solicitations to participate in research questionnaires, research studies, and clinical trials. (*Id.*) Plaintiff was surprised and troubled that information she believed she was communicating only to Defendant for the purpose of obtaining medical treatment had been sent to Facebook, Google, and other third parties. To remedy these violations, Plaintiff accordingly brings claims on her own behalf and on behalf of a Class of similarly situated persons. Santa Clara has moved to dismiss her claims, arguing that federal jurisdiction does not exist and that Santa Clara, as a government entity, is not subject to any of Plaintiff's causes of action except her CMIA claim.

IV. ARGUMENT AND AUTHORITIES

A. The Court has original jurisdiction over this case under CAFA.

When Santa Clara thought it could win a motion to dismiss Plaintiff's claims, it was delighted to subject itself to the Court's jurisdiction, take advantage of the Court's more rigorous pleading standards, and ask the Court to end Plaintiff's lawsuit before it began. After losing its first motion to dismiss, however, Santa Clara now apparently eregrets that choice, and asks the Court to send this case to a different judge, in a different venue. Santa Clara's transparent gamesmanship should be rejected.

1. Santa Clara's CAFA challenge is legally and factually deficient.

CAFA confers original jurisdiction over class actions involving (1) an aggregate amount in controversy of at least $5,000,000; (2) a class of more than 100 members; and (3) minimal diversity, *i.e.,* where at least one plaintiff and one defendant are citizens of different states. 28 U.S.C. § 1332(d)(2). Santa Clara does not dispute that this case involves a potential class of more than 100 members or that the amount in controversy exceeds the jurisdictional threshold. Instead, Santa Clara brings a "facial" challenge premised on the "home state exception" to CAFA, contending (falsely) that Plaintiff's complaint should be dismissed because minimal diversity is lacking. Mot. 3 ("Plaintiff's pleadings and government claim, however, facially allege an exception to CAFA jurisdiction that manages dismissal.").

While Santa Clara mistakenly styles its motion to dismiss as an attack on this Court's "subject matter jurisdiction," (Mot. 3-4), CAFA provides that "[a] district court shall decline to exercise jurisdiction" if either the "local controversy" or "home state" exceptions apply. 28 U.S.C. § 1332(d)(4). The provision providing that a district court shall decline to exercise jurisdiction operates as an abstention doctrine and does not divest the district court of subject matter jurisdiction. *Serrano v. 180 Connect, Inc*., 478 F.3d 1018, 1022 (9th Cir. 2007) ("Implicit in [CAFA] is that the court has jurisdiction, but the court either may or must decline to exercise such jurisdiction."); *Graphic Comm'ns Loc. 1B Health & Welfare Fund A v. CVS Caremark Corp*., 636 F.3d 971, 973 (8th Cir. 2011) ("[T]he local controversy provision operates as an abstention doctrine, which does not divest the district court of subject matter jurisdiction.").

As the party seeking dismissal, Santa Clara "bears the burden of proof" on *every* element of the home state exception. *Serrano*, 478 F.3d at 1024; *Jeter v. Wild W. Gas, LLC*, 2014 WL 3890308, at *5 (N.D. Okla. Aug. 7, 2014) ("As the parties invoking the CAFA exceptions, Defendants bear the burden of proving each element of the CAFA exceptions."). Further, CAFA does not say that dismissal under a statutory exception can be based simply on the allegations in a plaintiff's complaint. *Mondragon v. Cap. One Auto Fin*., 736 F.3d 880, 884 (9th Cir. 2013). Rather, a district court must make "factual findings regarding jurisdiction under a preponderance of the evidence standard." *Id.* As the Ninth Circuit has observed, "[a] complete lack of evidence does not satisfy this standard." *Id.* That is fatal to Santa Clara's motion.

First, Santa Clara argues that the "home-state controversy exception applies" because "*the proposed plaintiff class includes only California citizens*." Mot. 5 (emphasis in original). That is false. Plaintiff defined the "proposed class" as "all patients or prospective patients of Santa Clara Valley Medical Center … who exchanged communications at Santa Clara Valley Medical Center's websites." FAC ¶ 335. But treating with a California hospital "is not equivalent to citizenship." *Ehrman v. Cox Commc'ns, Inc*., 932 F.3d 1223, 1227 (9th Cir. 2019) ("We agree that residency is not equivalent to citizenship."). Likewise, Santa Clara ignores that Plaintiffs specifically pled that CAFA jurisdiction was appropriate because "at least one Class Member is a citizen of a different

state from Defendant." FAC ¶ 11. Because Santa Clara asserts a "facial" challenge to the Court's jurisdiction—i.e., a challenge that accepts the truth of the complaint's allegations but asserts they are insufficient on their face to invoke federal jurisdiction—Plaintiff's allegations are "sufficient" to establish minimal diversity. *Ehrman*, 932 F.3d at 1228.

Second, without citing any relevant authority, Santa Clara argues that, when making its abstention decision, the Court should ignore the allegations in Plaintiff's complaint in favor of a stray sentence in Plaintiff's written claim to the County of Santa Clara, filed to comply with the California Government Claims Act. Mot. 7. But Santa Clara provides no argument or explanation for how Plaintiff's statement that she "intends to seek relief on her behalf and on behalf of all similarly situated California citizens," prevented Santa Clara from "adequately investigat[ing]" Plaintiff's claims. Mot. 7. Nor does Santa Clara cite any case that has ever held—as Santa Clara falsely suggests—that subsequently pleading a class action on behalf of all Santa Clara *patients* would represent "a radical departure" or an "entirely different set of facts" from the privacy claims outlined in Plaintiff's three-page notice letter. Mot. 8.

The California Government Claims Act is not a "Gotcha" or a commandment demanding perfect compliance. Because the purpose of the Act "is to give the government entity notice sufficient for it to investigate and evaluate the claim, not to eliminate meritorious actions, the claims statute should not be applied to snare the unwary where its purpose has been satisfied." *Stockett v. Ass'n of Cal. Water Agencies Joint Powers Ins. Auth.*, 34 Cal. 4th 441, 445–46 (2004) (quotations omitted). A proper claim need not contain the detail and specificity required of a pleading, but need only "fairly" describe" what the entity is alleged to have done. *Stevenson v. San Francisco Hous. Auth.*, 24 Cal. App. 4th 269, 278 (1994) (holding additional allegations in complaint were not based on a different set of facts from those set out in the claim and were fairly included within the facts first noticed in the claim). Consequently, only "where there has been a *complete shift in allegations*, usually involving an effort to premise civil liability on acts or omissions committed at different times or by different persons than those described in the claim,

have courts generally found the complaint barred." *Stockett*, 34 Cal. 4th at 447 (emphasis added). Nothing of the sort is alleged here by Santa Clara. Nor could it be.

Plaintiff's complaint is predicated on the same fundamental privacy violations that are alleged in her written claim (*i.e.* the unauthorized disclosure of patients' communications to Facebook and Google via tracking technologies).[2] That is all the Government Claims Act requires. *Robinson v. Pickett*, 16 F. App'x 577, 581 (9th Cir. 2001) (holding Government Claims Act requires only that claim provide "adequate notice" of alleged causes of action). Santa Clara cites no cases holding to the contrary, much less any cases attempting to apply California Government Code section 910 in the context of making a determination about whether a complaint should be dismissed pursuant to the "home state exception" found in 28 U.S.C. § 1332(d)(4).

Finally, without any evidence, Santa Clara also simply *asserts* that "more than two-thirds of the proposed plaintiff class in this case are California citizens." But bald assertions are insufficient to meet Santa Clara's burden to show by a "preponderance of the evidence" that the home state exception applies. *King v. Great Am. Chicken Corp, Inc.*, 903 F.3d 875, 876 (9th Cir. 2018) ("Because there was no other evidence before the district court on that subject, the finding that more than two-thirds of the putative class members were citizens of California at the time of removal was clearly erroneous."). Because a "jurisdictional finding of fact should be based on more than guesswork," *Mondragon*, 736 F.3d at 884, Santa Clara's motion should be denied.

2. Santa Clara waived its CAFA arguments by waiting more than a year to bring its facial challenge to this Court's jurisdiction.

Although there is no statutory time limit, a party like Santa Clara must raise the home state exception "within a reasonable time" or the challenge is waived. *Barfield v. Sho-Me Power Elec. Co-op.*, 2014 WL 1343092, at *2 (W.D. Mo. Apr. 4, 2014) (finding twenty-six month delay

[2] *See* Dkt. 70-1 at 4 ("Santa Clara Valley Medical Center discloses **its patients'** PHI and PII through the deployment of various digital marketing and automatic rerouting tools embedded on its website and patient portal that purposefully and intentionally redirect personal health information to Facebook and Google, who exploit that information for advertising purposes.") (emphasis added).

unreasonable where discovery has been extensive and parties had "invested hundreds of hours on motions to dismiss, a motion to sever, issues of class certification, and motions for summary judgment, as well as many ongoing procedural details"). And while "what is reasonable will vary according to the relevant facts, it is preferable that such motions be made at the earliest practical time." *Martin v. Trott L., P.C.*, 265 F. Supp. 3d 731, 745 (E.D. Mich. 2017) (denying defendant's CAFA challenge made after defendant had previously filed and lost a motion to dismiss).

Here, Santa Clara's motion to dismiss pursuant to the home state exception was not made within a reasonable time and is therefore waived. More than a year has passed since Plaintiff filed her original complaint in federal court alleging CAFA jurisdiction, (Dkt. 1), and almost five months have passed since the Court informed Santa Clara at the April 9, 2024 status conference that discovery would proceed because Plaintiff had sufficiently alleged her claims. Santa Clara offers no argument or excuse for why it waited more than a year to make a facial challenge to the Court's jurisdiction. That is woefully insufficient. *See, e.g., Calingo v. Meridian Res. Co.* LLC, 2011 WL 3611319, at *6 (S.D.N.Y. Aug. 16, 2011) ("[W]ithout an argument regarding the reason for the delay, the Court believes 87 days is too long and is unreasonable.").

Unlike cases where Defendants timely moved to contest CAFA jurisdiction because of newly discovered facts, nothing prevented Santa Clara from challenging this Court's jurisdiction more than a year ago. None of the relevant allegations in Plaintiff's complaint have changed. No new "facts" have come to light during discovery. The only thing that has changed is that the Court denied Santa Clara's prior motion to dismiss and informed Santa Clara that discovery would proceed. But dissatisfaction with a Court's rulings is not an acceptable excuse for unreasonably delaying a CAFA challenge under federal precedent. Because Santa Clara "has not provided a persuasive reason for its lengthy delay," *Barfield*, 2014 WL 1343092, its untimely challenge should be denied.

Moreover, Santa Clara's assertion that this Court lacks jurisdiction is inconsistent with the position it took earlier in the case. Previously, Santa Clara invoked the authority of the Court to adjudicate this case when it moved for dismissal under Rule 12(b)(6), asking the Court to exercise

jurisdiction, grant its dispositive motion, and render judgment in Santa Clara's favor on the merits. Had the Court ruled in Santa Clara's favor, there is no doubt that Santa Clara would not now be challenging the Court's CAFA jurisdiction. Rather, Santa Clara's decision to delay raising this issue strongly suggests a litigation strategy to wait until the Court had ruled on the first motion to dismiss before challenging jurisdiction. Federal courts frown upon such gamesmanship. *Meadows v. Bicrodyne Corp*., 785 F.2d 670, 672 (9th Cir. 1986) ("Appellants, by appearing repeatedly before the court before raising the [jurisdiction] objection, … waived their right to raise that issue."); *Bearden v. PNS Stores, Inc*., 894 F.Supp. 1418, 1424 (D. Nev. 1995) (plaintiffs waived their right to remand by "filing numerous pleadings and discovery requests after the case was removed to this federal court"). Because "a party that wants a federal court to decline jurisdiction under one of CAFA's exceptions must timely assert his objection," Santa Clara's decision to intentionally delay its CAFA challenge until after the Court had ruled on its 12(b)(6) motion means that Santa Clara "may not raise it" now. *Martin*, 265 F. Supp. 3d at 745.

The parties have collectively spent hundreds of hours briefing motions to dismiss, attending status conferences, and engaging in written discovery. Indeed, Santa Clara has already forced Plaintiff to respond to 39 requests for production and 22 interrogatories, while requiring Plaintiff to engage in multiple meet and confers over the last six months to obtain even basic discovery from Santa Clara. Forcing Plaintiff to start her lawsuit all over again in a different court more than a year after the case was filed is obviously prejudicial to Plaintiff and would serve no purpose other than further delay.

Santa Clara certainly had access to all the facts necessary to make its CAFA challenge more than a year ago. Santa Clara has not given any reason why it could not have timely raised, at the very outset of this case, the same arguments it now makes, based on the same facts on which it now relies. Because there is "no basis in the present record to apply CAFA's home state exception" based on Santa Clara's "tardy request," *Martin*, 265 F.Supp.3d at 745, this Court should deny Santa Clara's untimely challenge.

B. This Court has federal question jurisdiction under the Federal Wiretap Act.

Even if Santa Clara's challenge to CAFA diversity jurisdiction were proper, this Court should retain jurisdiction over this case under 28 U.S.C. § 1331 because Plaintiff has pled a claim under the Federal Wiretap Act, 18 U.S.C. § 2511(1) et seq., giving rise to federal question jurisdiction. Seeking to defeat federal question jurisdiction as well as liability under the Wiretap Act, Santa Clara asks this Court to endorse the proposition that county-owned hospitals are free to wiretap their patients' communications (and then barter those communications to Facebook and Google) without patients' consent. Mot. 9-13. Specifically, Santa Clara argues that Plaintiff's wiretapping claim should be dismissed because local government entities such as Santa Clara Valley Medical Center and the County of Santa Clara do not fall within the ambit of Section 2511(1) of the Electronic Communications Privacy Act. Mot. 9-12. That argument fails for multiple reasons.

First, as Santa Clara itself admits, (Mot. 11), the ECPA's Section 2511(3)(a) does create a substantive right against government entities that provide an "electronic communications service," as Santa Clara does through its patient portal. Santa Clara nevertheless suggests that Plaintiff's ECPA claim can be solely cabined to 18 U.S.C. § 2511(1). But that argument not only ignores Plaintiff's allegations, but also disregards the standards and presumptions that this Court applies when deciding a motion to dismiss.

Second, Santa Clara's principal argument—*i.e.* that wiretapping victims have no "substantive rights" against "governmental entities" who disclosure their intercepted communications—is premised on a profound misunderstanding of both the language and the structure of the ECPA. In 18 U.S.C. § 2520(g), the ECPA provides a right of action against a "governmental entity" that willfully discloses communications beyond the extent permitted by Section 2517 (a series of exceptions allowing law enforcement officers to disclose lawfully intercepted communications). Because Santa Clara's interpretation would essentially nullify this provision, the Court should reject it and instead follow the majority view.

1. Governmental entities like Santa Clara fall within the ambit of 18 U.S.C. § 2520(a)'s creation of a civil action for wiretapping.

The ECPA provides that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person **or entity**, other than the United States, which engaged in that violation such relief as may be appropriate." 18 U.S.C.A. § 2520(a) (emphasis added). While there is a split in authority about the meaning of the term "entity," the "majority view" is that Congress intended to make governmental entities like the County of Santa Clara liable under the ECPA. *See Kemeness v. Worth Cnty., Georgia*, 449 F. Supp. 3d 1318, 1324 (M.D. Ga. 2020) (collecting cases). Even *Seitz*, the case on which Santa Clara primarily relies, agrees with this analysis. *Seitz v. City of Elgin*, 719 F.3d 654, 657 (7th Cir. 2013) ("[W]e agree with plaintiffs that 'entity' as used in § 2520(a) includes government units."). So do several of the California federal district court opinions Santa Clara cites. *See Medina v. Cnty. of Riverside*, 2006 WL 8437749, at *4 (C.D. Cal. Dec. 1, 2006) ("The federal wiretap statutes are applicable to counties and other governmental entities."); *Federated Univ. Police Officers' Ass'n v. Regents of Univ. of California*, 2015 WL 13273308, at *8 (C.D. Cal. July 29, 2015) ("'[E]ntity" as used in § 2520 includes government units"). The majority is correct.

Congress passed the Wiretap Act in 1968 as part of the Omnibus Crime Control and Safe Streets Act, making it a crime for "any person" to "willfully" intercept, endeavor to intercept, or procure "any other person to intercept or endeavor to intercept, any wire or oral communication." Pub. L. No. 90-351, § 802, 82 Stat. 197, 223 (1968) (codified as amended at 18 U.S.C. § 2511(1)). The Act included a civil remedies provision, codified at 18 U.S.C. § 2520, which allowed an individual whose communications are intercepted in violation of the Act to bring a private cause of action against any "person" responsible for such violations.

When Congress passed the Electronic Communications Privacy Act of 1986, however, section 2520 was amended to provide that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person *or entity* which engaged in that violation such relief as may

be appropriate." Pub. L. No. 99-508, § 103, 100 Stat. 1848, 1854 (1986) (emphasis added). Congress amended this section again in 2001, excluding the United States from liability as an "entity." USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 223(a)(1), 115 Stat. 272, 293.

As the Sixth Circuit explained in *Adams v. City of Battle Creek*, 250 F.3d 980, 985 (6th Cir. 2001) "[t]he addition of the words "entity" can only mean a governmental entity because prior to the 1986 amendments, the definition of 'person' already included business entities." 250 F.3d at 985. If "entity" in this part of the statute was meant only to refer to business entities, then it would be redundant or superfluous, in violation of the basic rules of statutory construction. *Id.* This interpretation is further bolstered by the 2001 amendment, which added "other than the United States" immediately after "entity," evincing Congress's intent to exclude the United States—but not any other governmental entities—from the list of entities the statute covers. "There would have been no reason for Congress to carve out an exception for the United States if governmental entities could not be sued under the statute." *Garza v. Bexar Metro. Water Dist*., 639 F. Supp. 2d 770, 774 (W.D. Tex. 2009) (citing *Williams v. City of Tulsa, OK*, 393 F. Supp. 2d 1124, 1133 (N.D. Okla. 2005)).

2. Plaintiff has stated valid wiretapping claims for violation of the substantive rights created against governmental entities in 18 U.S.C. § 2511(3)(a).

As Santa Clara concedes, the ECPA creates a substantive right against governmental agencies that provide electronic communications services pursuant to 18 U.S.C.§ 2511(3)(a). Mot. 11 ("[T]he FWA creates a substantive right against a government entity … in section 2511(3)(a)."). Plaintiff alleges that Santa Clara's installation of tracking software in its patient portal violated this Section.

Section 2511(3)(a) provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication … while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication." "Electronic communications service" is defined by the ECPA to mean "*any service* which provides to users thereof the ability to send or receive wire or electronic

communications." 18 U.S.C. § 2510(15) (emphasis added). And section 2510(12) defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12).

Santa Clara provides such an "electronic communication service" to its patients via its patient portal. Plaintiff's FAC alleges that Santa Clara's patient portal offers a variety of communications services, including allowing Plaintiff to "access her lab results, schedule doctor's appointments, refill prescriptions, and communicate with her doctors." FAC ¶ 20. Plaintiff alleges that tracking pixels in the web based version of the patient portal disclosed these communications to Facebook and Google. FAC ¶ 33. These functions are also available via Santa Clara's patient portal mobile app, which Plaintiffs allege contains Google Firebase code that discloses patients' communications to Google. FAC ¶¶ 34-35.[3] Unbeknownst to patients, the installation of this code inside the Santa Clara patient portal app resulted in disclosures of patients' personal health information, including their patient status, whenever they logged into the app." FAC ¶¶ 34-35. Plaintiff further alleges that the Firebase code incorporated into Santa Clara's mobile app enabled Google "to collect information such as a user's age bracket, gender, interests, device brand, device category, location, operating system, and other information regarding users' interactions with the

[3] Contrary to Santa Clara's arguments, Plaintiff's allegations regarding the mobile app are not a new claim, (Mot 18), but merely an elaboration on Plaintiff's claims regarding Santa Clara's patient portal. *See Frazier v. City of Fresno*, No. 20-cv-1069, 2023 WL 4108322, at *29 ("Where the complaint merely elaborates or adds further detail to a claim, but is predicated on the same fundamental actions or failures to act by the defendants, courts have generally found the claim fairly reflects the facts pled in the complaint." (citing *White v. Superior Court*, 225 Cal. App. 3d 1505, 1510–1511(1990)); *Blair v. Superior Court*, 218 Cal. App. 3d 221, 226 (1990) (finding that new allegations regarding county's negligence were not barred where pre-suit claim "may reasonably be read to encompass" the factual details added in the court-filed complaint). The mobile app is simply another means of accessing Santa Clara's patient portal, and Plaintiff's addition of details regarding how Santa Clara used tracking software to disclose patient portal communications made via the mobile app merely elaborates on the "various digital marketing and automatic rerouting tools embedded on [Santa Clara's] website and patient portal that purposefully and intentionally redirect personal health information to Facebook and Google," which Plaintiff notified Santa Clara were the basis of her claim before filing suit. Dkt. 70-1 at 4.

app." FAC ¶ 35. This surreptitious Firebase Code also allowed Google to collect "text that users type into an app; track results of users' searches within an app; and track users' downloads of files within an app." FAC ¶ 35. Such electronic "signs," "data," and "writing" satisfy the definition of "electronic communication" provided in 18 U.S.C. § 2510(12).

The ECPA defines an electronic communications service as *any* service that allows users to send and receive electronic communications. On its face, the patient portal that Santa Clara offers patients is a "service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Santa Clara's patient portal provides a "service" that enables patients and their doctors to communicate with each other. FAC ¶ 33 (alleging that Plaintiff used patient portal to send and receive messages regarding sensitive medical issues). Like the web-based patient portal app, the mobile portal app also allows patients to schedule appointments, renew prescriptions, pay bills, access lab results, and message their doctors. FAC ¶¶ 17, 35. The patient portal thus squarely fits the ECPA's definition of an "electronic communications service." *TLS Management LLC v. Rodriguez-Toledo*, 260 F. Supp. 3d 154, 160 (D.P.R. 2016) (holding that Dropbox was an "electronic communications service" where the plaintiffs alleged that it "allows users to send content filled 'files' and 'documents' over the Internet."); *see Ehling v. Monmouth-Ocean Hosp. Serv. Corp*., 961 F. Supp. 2d 659, 667 (D.N.J. 2013) (holding Facebook's messaging application qualified as an "electronic communications service"); *Crispin v. Christian Audigier, Inc*., 717 F. Supp. 2d 965, 981 (C.D. Cal. 2010) (holding that Facebook and MySpace bulletin board applications qualified as "electronic communications service"); *In re United States for Prtt Ord. for One Whatsapp Chief Acct. for Investigation of Violation of 21 U.S.C. § 841*, No. 18-PR-00017, 2018 WL 1358812, at *5 (D.D.C. Mar. 2, 2018) (holding that Whats App application qualified as an "electronic communications service"); *Inventory Locator Serv., LLC v. Partsbase, Inc*., 2005 WL 2179185, at *24 (W. D. Tenn. Sept. 6, 2005) (holding password protected electronic bulletin board and web-based forum qualified as "electronic communications service"); *see also Quon v. Arch Wireless Operating Co*, 529 F.3d 892,

901 (9th Cir. 2008) (rev'd on other grounds) (text-messaging pager services quailed as "electronic communications service").

Plaintiff alleges that Santa Clara violated the ECPA by intentionally divulging the contents of her and her fellow patients' communications without consent via surreptitious tracking code that was deployed on the patient portal web app and Santa Clara mobile app. FAC ¶¶ 32-35, 353, 356, 375. For example, Plaintiff alleges that "Defendant, through the source code it deployed and ran on its … mobile app, contemporaneously and intentionally redirected the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including … and Google." FAC ¶ 356. Plaintiff further alleges that "Defendant's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff's and Class Members' regarding PII and PHI, treatment, medication, and scheduling." FAC ¶ 357. Finally, Plaintiff also alleges that Santa Clara *intentionally* shared her communications with Google as part of illegal scheme to benefit Santa Clara. FAC ¶¶ 50-55, 60, 375. These allegations state a valid claim ECPA claim against Santa Clara as a governmental "entity" providing an electronic communications service. *See* 18 U.S.C. § 2511(3)(a) (prohibiting a "person or *entity*" providing an electronic communication service from "intentionally divulg[ing] the contents of any communication") (emphasis added).

Santa Clara does not suggest that Plaintiff failed to sufficiently plead facts in support of her ECPA claim. Rather, Santa Clara argues that the Court should find that Plaintiff's claim is *cabined* to 18 U.S.C. 2511(1), which therefore (according to Santa Clara) excuses Santa Clara from any liability under the ECPA. Mot. 12-13. That argument, however, ignores both what Plaintiff pled and the relevant pleading standard.

Plaintiff's ECPA claim is not limited to just section 2511(1). Rather, Plaintiff pled a cause of action for "**VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 18 U.S.C § 2511(1) *ET SEQ.* UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSOURE.**" FAC (Count I). In other words, Plaintiff alleged a claim against Santa

Clara for violating the ECPA—not just the specific sections of the ECPA found in 18 U.S.C. § 2511(1). For example, Plaintiff specifically plead that "18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used **in violation of Chapter 119.**" FAC ¶ 347. "Chapter 119" refers to the entire chapter of the United States Criminal Code addressing "Wire and Electronic Communications Interception and Interception of Oral Communications." *See* 18 U.S.C. Pt. 1, Ch. 119, Refs. & Annos. That chapter encompasses 18 U.S.C. § 2510 to 18 U.S.C. § 2523.

While it is understandable that Santa Clara would like the Court to disregard the other relevant sections of the Act—especially 18 U.S.C. § 2511(3) and 18 U.S.C. § 2517, which provide additional predicates for the causes of action authorized by 18 U.S.C. § 2520(a) & (g)—the Court is obligated to "construe the pleadings in the light most favorable to the nonmoving party," *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir.2008), while "drawing all 'reasonable inferences' in the nonmoving party's favor." *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001).

Plaintiff was not required to plead "something more" than the Electronic Communications Privacy Act in setting out her claims against Santa Clara. *Fontana v. Haskin*, 262 F.3d 871, 877 (9th Cir. 2001) ("Specific legal theories need not be pleaded so long as sufficient factual averments show that the claimant may be entitled to some relief."); *Sagana v. Tenorio*, 384 F.3d 731, 737 (9th Cir. 2004) ("We long ago rejected the argument that a specific statute must be named, describing it as an "attempt to evoke wholly out-moded technical pleading rules."); *Seal Source, Inc. v. Calderon*, 2010 WL 3122836, at *2 (D. Or. Aug. 27, 2009) ("Defendant cites no authority for the proposition that Seal Source is required to plead 'something more'" than "the Computer Fraud and Abuse Act, 18 U.S.C. § 1030" to "give notice of the court's jurisdiction.").

Having pled "sufficient factual averments" to show that she "may be entitled to some relief," including specific factual allegations demonstrating that she is entitled to relief under 18 U.S.C. § 2511(3), Plaintiff has more than satisfied her burden. *Consumer Fin. Prot. Bureau v. Prime Mktg. Holdings, LLC*, 2017 WL 2772313, at *11, n.3 (C.D. Cal. Jan. 19, 2017) ("[S]o long

as Plaintiff's FAC pleads sufficient facts to support a net impression theory, it may proceed on this basis."). Accordingly, Santa Clara's motion to dismiss Plaintiff's ECPA claim should be denied.

3. Plaintiff has also stated valid claims pursuant to 18 U.S.C. § 2520(a), 18 U.S.C. § 2520(g), 18 U.S.C. § 2517, and 18 U.S.C. § 2511(1).

Santa Clara also mistakenly suggests that the "only" substantive provision in ECPA authorizing a cause of action against a governmental entity is 18 U.S.C. § 2511(3)(a). Mot. 10-11. Not so. Because Congress also created a cause of action against a "governmental entity" that willfully discloses illegally wiretapped information under 18 U.S.C. § 2520(g), the only consistent reading of the ECPA as a whole is that its prohibitions of illegal wiretapping apply to willful disclosures by counties, such as Plaintiff alleges here.

Congress originally passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. §§ 2510–23, in 1968. Title III established a "comprehensive scheme for the regulation of wiretapping and electronic surveillance." *Gelbard v. United States*, 408 U.S. 41, 46 (1972). Congress enacted Title III to (1) protect the privacy of wire and oral communications, and (2) delineate on a uniform basis "the circumstances and conditions under which the interception of wire and oral communications may be authorized." *Id.* at 48 (quoting S. Rep. No. 1097, at 66, reprinted in 1968 U.S.C.C.A.N. 2112, 2153). Under Title III, law enforcement can intercept private wire and oral communications only to investigate serious crimes and with prior judicial approval. *Id*. Intentionally intercepting wire, oral, or electronic communications without authorization under Title III, however, is illegal. *See* 18 U.S.C. § 2511(1). So is intentionally disclosing the contents of unauthorized intercepts. *Id.*

But the fruits of lawful wiretaps can be used or disclosed in limited circumstances. *See* 18 U.S.C. § 2517. For example, an "investigative or law enforcement officer who, by any means authorized by [Title III], has obtained knowledge" of a wiretap's contents can use the information or disclose it to another officer when doing so is "appropriate to the proper performance" of their "official duties." 18 U.S.C. § 2517(1), (5). Likewise, an "investigative officer" who, by any means authorized by Title III, "has obtained knowledge of the contents of any wire, oral, or electronic

communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties." 18 U.S.C.A. § 2517(2). Disclosure is also lawful when national security is at risk. *See* 18 U.S.C. § 2517(6), (8).

In 2001, Congress amended Title III to provide civil liability for *willful* violations of section 2517. Specifically, under 18 U.S.C. § 2520(g), "[a]ny willful disclosure or use by an investigative or law enforcement officer **or governmental entity** of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)." Much as section 2511(2) creates a series of exceptions to the general rule that electronic communications cannot be "intercepted" without prior consent, section 2517 creates a series of exceptions to general rule that electronic communications cannot be "disclosed" by government entities and their agents without prior consent from all parties. A government entity who discloses communications "beyond the extent permitted" by § 2517, however, violates § 2520(g). For example, a "governmental entity" like Santa Clara who discloses electronic communications that have been acquired by a means that is *not* authorized by the ECPA (like bugging criminal suspects without a warrant or installing surreptitious tracking technologies on the public's phones) is liable to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

Moreover, the limitations on a governmental entity's authorization to wiretap the public are not just those in Section 2517. Because section 2517 expressly incorporates the protections afforded by the rest of the ECPA, it incorporates the specific substantive rights set forth in 18 U.S.C. §§ 2511(1) and 2511(2). *See, e.g.,* 18 U.S.C. § 2517(1) (permitting investigative officer to disclose "contents" of communications that have been obtained "by any means authorized by this chapter"); 18 U.S.C. § 2517(2) (permitting use of "any wire, oral, or electronic communication" that an officer has obtained "by any means authorized by this chapter"). In other words, disclosing electronic communications that have been obtained in violation of the prohibitions elsewhere in the chapter—like 18 U.S.C. § 2511(1)—would be a violation of 18 U.S.C. § 2517, triggering liability under the ECPA. For example, while a government entity may lawfully employ "pen

registers" pursuant to 2511(2)(h), it may do so only if its agents have obtained lawful warrants pursuant to Chapter 206 of the United States Criminal Code.

Contrary to Santa Clara's argument, the ECPA does not exempt *counties* from the very same liabilities that a *county's employees* are liable for if they violate the ECPA. Rather, the ECPA imposes a specific limitation on liability for "governmental entities" in 18 U.S.C. § 2520(g). Specifically, section 2520(g) provides that, to establish liability against a governmental entity, a plaintiff must demonstrate that the governmental entity "*willfully* used the wiretap information in violation of Title III." *B & G Towing, LLC v. City of Detroit, MI*, 828 F. App'x 263, 267 (6th Cir. 2020) (emphasis in original) (recognizing governmental entities like cities may be liable pursuant to 18 U.S.C. § 2520(g)). As the Sixth Circuit has explained, "willfully" in section 2520(g) means "knowingly or recklessly" disregarding for "a known legal duty."

Here, Plaintiff has more than sufficiently alleged that Santa Clara both "knowingly" and "recklessly" disregarded a host of legal duties to Plaintiff and her fellow class members. *See* FAC §§ 4, 41, 367-376. For example, Plaintiff specifically pled that notwithstanding "Santa Clara's legal duties of confidentiality Santa Clara disclosed (and continues to disclose) the contents of Plaintiff's and Class Members' communications and protected health information via automatic tracking mechanisms embedded in the websites operated by Santa Clara without patients' knowledge, authorization, or consent." FAC ¶ 50. Likewise, Plaintiff alleges that, despite its legal privacy obligations, Santa Clara failed to take steps to block the transmission of its patients' health information to Facebook and Google or to warn patients that Santa Clara was routinely bartering their health information to tech companies. FAC ¶ 58. Plaintiff further alleged that, despite its knowledge that HIPAA expressly forbids sharing patients' IP addresses and other personal identifiers without authorization, Santa Clara did so anyway because it wanted access to the marketing and analytics benefits provided by Facebook and Google. FAC ¶¶ 60, 113-120, 207-213, 223-224, 247; FAC ¶ 248 ("Santa Clara intentionally shared the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool."); FAC ¶ 258 ("Santa Clara *willfully* chose to implement Meta Pixel on its websites and aid in the

disclosure of personally identifiable information and sensitive medical information about its patients … to third parties, including Facebook and Google.") (emphasis added).

Plaintiff also laid out the legal duties that Santa Clara chose to disregard in the pursuit of profit. *See* FAC ¶¶ 288-293; 364-377. Those duties include the specific criminal provisions in HIPAA prohibiting a heath care provider like Santa Clara from unauthorized use of "individually identifiable health information for commercial advantage." FAC ¶¶ 368-371 (discussing Santa Clara's violations of 42 U.S.C. § 1320d-6). As multiple courts have recognized, disclosing patients' health data for advertising purposes facially violates 42 U.S.C. § 1320d-6, implicating the crime-tort exception in the ECPA. *See Brahm v. Hosp. Sisters Health Sys*., 2024 WL 3226135, at *6 (W.D. Wis. June 28, 2024) ("[T]he court finds that plaintiff has plausibly alleged that defendants' primary motivation in intercepting and disclosing patients' PII/PHI was to commit wrongful and tortious acts—namely the disclosure and use of patient data for advertising, marketing, and revenue generation without their express written consent."); *Kane v. Univ. of Rochester*, 2024 WL 1178340, at *7 (W.D.N.Y. Mar. 19, 2024) (same).

Plaintiff alleges that, despite Santa Clara's well known privacy obligations under state and federal law, Santa Clara chose "to hide its use of the Meta Pixel tool from its own patients even after learning that its patients' Personal Health Information was being routinely collected, transmitted, and exploited by Facebook." FAC ¶ 326; *see also* FAC ¶ 358 ("By intentionally disclosing … the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c)."). In short, Plaintiff alleges that Santa Clara "purposefully" violated HIPAA for its own financial gain. FAC ¶¶ 377-378. Those allegations are more than sufficient to show that Santa Clara "knowingly or recklessly" disregarded a "known legal duty." *B & G Towing,* 828 F. App'x at 267.

While Santa Clara is silent on § 2520(g) in its motion, it appears that Santa Clara's position that "only" § 2511(3) provides a substantive right of action against government entities is

predicated on the argument that 18 U.S.C. § 2517 does not specifically use the word "entity" in laying out when ECPA authorizes disclosure of intercepted communications. Any such argument, however, would violate basic rules of statutory construction.

Most fundamentally, when courts interpret a federal statute, one "basic rule" is that "one provision should not be interpreted in a way which is internally contradictory or that renders other provisions of the same statute inconsistent or meaningless. *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978). Another basic rule is that an Act like the Electronic Communications and Privacy Act, "should not be read as a series of unrelated and isolated provisions." *Gustafson v. Alloyd Co*., 513 U.S. 561, 570 (1995). In other words, courts must "interpret statutes as a whole, giving effect to each word and making every effort not to interpret a provision in a manner that renders other provisions of the same statute inconsistent, meaningless or superfluous." *Boise Cascade Corp. v. U.S. E.P.A*., 942 F.2d 1427, 1432 (9th Cir.1991).

Of course, accepting Santa Clara's interpretation would mean that 2520(g)'s imposition of liability on governmental entities who "willfully" disclose information "beyond the extent permitted by section 2517" would be nullified and rendered superfluous. On Santa Clara's cramped reading, because the word "entity" does not appear in section 2517, a "governmental entity" could *never* be liable pursuant to section 2520(g). Indeed, Santa Clara makes that argument expressly in connection with 18 U.S.C. § 2511(1). But that reading violates the basic obligation to read an Act like the ECPA as a whole. Because Santa Clara's interpretation would literally render the prohibition in section 2520(g) "inconsistent and meaningless," it must be rejected. And because section 2517 expressly incorporates the rest of the Act, including section 2511(1), Santa Clara's reading of section 2511(1) is equally dubious.

Further support for interpreting the ECPA to authorize claims against counties comes from a parallel provision of the Act: 18 U.S.C. § 2707(a). That section, which imposes civil liability for interception of stored wire and electronic communications, was also amended in 1986 to add "or entity" to the list of those who can be held civilly liable. The Senate report summarizing the changes to § 2707 specifically states that the word "entity" includes governmental entities. S. Rep.

No. 541, 99th Cong., 2d Sess. 43 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3597; *Adams*, 250 F.3d at 985. Because "entity" in § 2707(a) should be read *in pari materia* with "entity" in its sister provision § 2520(a), the meaning of the former strongly supports the case for governmental liability under the latter. See *Ala. Educ. Ass'n v. State Superintendent of Educ.*, 746 F.3d 1135, 1158 (11th Cir. 2014) ("[S]tatutes on the same subject matter should be construed together so as to harmonize them."). So too, it makes little sense that Congress would authorize broad liability for counties under the Stored Communications Act, but then simultaneously restrict such liability to a single provision in the Electronic Communications and Privacy Act. *See, e.g.*, *Kemeness*, 449 F. Supp. 3d at 1325 (holding "entity" in § 2520(a) should be read *in pari materia* with "entity" in § 2707(a)).

Read "as a whole," *Boise Cascade*, 942 F.2d at 1427, the better interpretation of the ECPA is that Congress intended governmental entities to have liability for the unauthorized disclosure of wire communications but *only to the extent* that such violations are *willful*. This interpretation, unlike that offered by Santa Clara, has the benefit of making sense of the Act as a whole. Further, it is congruent with the majority of courts, including the Sixth Circuit and Second Circuit, who have previously held that ECPA imposes liability on cities and counties. *See Adams*, 250 F.3d at 985 ("[W]e we hold that governmental entities may be liable under 18 U.S.C. § 2520); *Organizacion JD Ltda. v. U.S. Dep't of Just.*, 18 F.3d 91, 94 (2d Cir. 1994) ("[E]ntity must be taken to mean governmental entity."); *Medina v. Cnty. of Riverside*, 2006 WL 8437749, at *5 (C.D. Cal. Dec. 1, 2006) ("A plain reading of the statutory text reveals that the federal wiretap statutes are applicable to the County of Riverside.").

In short, Plaintiff has stated a valid wiretapping claim under the ECPA. The Court should therefore find that federal jurisdiction exists and deny Santa Clara's Motion to Dismiss.

C. Plaintiff has stated a viable California Government Code § 815.6 claim.

Because Plaintiff alleges that Santa Clara violated "mandatory duties" under HIPAA and its California analog, the CMIA, as well as the Federal Wiretap Act, the Court should also deny Santa Clara's Motion to Dismiss her claim under CAL. GOV'T CODE § 815.6.[4]

1. Santa Clara's violation of mandatory duties under HIPAA supports a § 815.6 claim.

The County claims that because there is no private right of action under HIPAA, the mandatory duties imposed by HIPAA cannot support a § 815.6 claim. Mot. 20–22. This is wrong as a matter of law. The Supreme Court of California has held that § 815.6 does not require that the source of a mandatory duty itself has a private right of action. *Haggis v. City of Los Angeles*, 22 Cal. 4th 490, 499, 993 P.2d 983, 988 (2000) ("We cannot agree . . . that liability under section 815.6 requires that the enactment establishing a mandatory duty *itself* manifest an intent to create a private right of action, for their position is directly contrary to the language and function of section 815.6.") (emphasis in original).

One of the key cases the County relies on to argue the opposite is an unpublished opinion that fails to cite *Haggis* altogether, much less reconcile *Haggis* with its reasoning. *See* Mot. 21 (quoting repeatedly *Delux Pub. Charter, LLC v. Cnty. Orange*, No. SACV202344JVSKESX, 2022 WL 18228386 (C.D. Cal. Oct. 31, 2022), *motion to certify appeal denied*, No. SACV202344JVSKESX, 2023 WL 2558784 (C.D. Cal. Jan. 11, 2023)).

The second, *Dep't of Corps. v. Superior Court*, 153 Cal. App. 4th 916, 935 (2007), is distinguishable. Mot. 21. First, there was an independent basis to prohibit a § 815.6 claim there: the relevant statute provided "'pervasively discretionary' authority" for its enforcement, rather than imposed a mandatory duty. 153 Cal. App. at 931–33 (quoting *Haggis*, 22 Cal. 4th at 506). HIPAA confidentiality requirements are not "discretionary," and the County nowhere argues that they are. *See* Mot. 20–21.

[4] Plaintiff will not rely on the California Consumer Privacy Act, CAL. CIV. CODE § 1798.100, or statutory fraud, CAL. CIV. CODE §§ 1709 and 1710, to support her § 815.6 claim.

Second, there was express language in the disputed statute that limited when private causes of action were permissible, and no such language here. *Dep't of Corps.*, 153 Cal. App. 4th at 934 ("except as 'explicitly provided,' no civil liability in favor of 'any private party' shall arise against 'any person'") (citation omitted). The Court applied the canon that the specific governs the general to construe the statutes together and find § 815.6 not viable. *See id.* at 934 (citing *Arbuckle–College City Fire Protection Dist. v. County of Colusa*, 105 Cal. App. 4th 1155, 1166 (2003) ("Generally, it can be presumed that when the Legislature has enacted a specific statute to deal with a particular matter, it would intend the specific statute to control over more general provisions of law that might otherwise apply"). There is no such controlling express language in HIPAA. As the County concedes, there is a negative implication that federal authorities intended only the Secretary of Health and Human Services to enforce HIPAA. *See* Mot. 22 (collecting cases). Construing the statutes together here, the Court should not allow a negative implication to overcome the express language of § 815.6. *See In re J.W.*, 29 Cal. 4th 200, 209, 57 P.3d 363, 369 (2002) ("courts do not apply the *expressio unius est exclusio alterius* principle 'if its operation would contradict a discernible and contrary legislative intent.'") (citations omitted). To do so would violate the "language and function of section 815.6" of requiring California public entities to comply with mandatory duties with reasonable diligence. *Haggis*, 22 Cal. 4th 499–500.

In sum, a statute that puts a "public entity under an obligatory duty to act or refrain from acting, with the purpose of preventing the specific type of injury that occurred" permits "liability [] against the agency under section 815.6, regardless of whether private recovery liability would have been permitted . . . under the predicate enactment alone." *Haggis*, 22 Cal. 4th at 500. The County disregards this law and has no other basis to challenge the HIPAA predicate for the § 815.6 claim. *See* Mot. 20–22. Its motion to dismiss on this basis should therefore be denied.

2. Santa Clara's violation of mandatory duties under the CMIA also supports a § 815.6 claim.

The County argues the CMIA predicate for the § 815.6 claim "is impermissibly duplicative" of the separate CMIA claims in the FAC. Mot. 22. The County says there are "no new

allegations about the County's obligations, the County's supposed breach, or Plaintiff's claimed damages." *Id.* This is not correct, because the burdens of proof are not identical between the causes of action, as properly alleged in the FAC. Under the CMIA, the case in chief requires proof of scienter. *See* CAL. CIV. CODE § 56.101(a) ("any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information"); CAL. CIV. CODE § 56.36 (permitting different remedies for negligent, knowing, and willful violations). In contrast, under § 815.6, the burden is on the public entity to prove it exercised reasonable diligence when it failed to comply with a mandatory duty. *See, e.g.*, CAL. GOV'T CODE § 815.6 ("unless ***the public entity establishes*** that it exercised reasonable diligence to discharge the duty") (emphasis added). Since the different causes of action require different burdens of proof, they are not duplicative, and the § 815.6 claim should not be dismissed.

3. Santa Clara's violation of mandatory Wiretap Act duties also supports the § 815.6 claim.

Plaintiff's alleged Wiretap Act violations also show alleged violations of "mandatory duties" giving rise to a claim under § 815.6 *See supra* Section IV.C.2 Moreover, the § 815.6 claim is not duplicative of the Wiretap Act claim because the burdens of proof for these claims are not identical, for the same reasons explained above. *See supra* Section IV.B; *contra* Mot. 24. The Court should therefore allow Plaintiff to proceed with her claim under Section 815.6.

V. CONCLUSION

For the reasons stated above, the Court should deny Santa Clara's Motion to Dismiss.

Dated: September 20, 2024

Respectfully submitted,

By: */s/ Michael A. Caddell*

Michael A. Caddell (SBN 249469)
mac@caddellchapman.com
Cynthia B. Chapman (SBN 164471)
cbc@caddellchapman.com
Amy E. Tabor (SBN 297660)
aet@caddellchapman.com
CADDELL & CHAPMAN
628 East 9th Street
Houston TX 77007-1722
Tel.: (713) 751-0400
Fax: (713) 751-0906

Foster C. Johnson (SBN 289055)
AHMAD, ZAVITSANOS, & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston TX 77010
(713) 655-1101
fjohnson@azalaw.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I, Amy E. Tabor hereby certify that on September 20, 2024 this document was filed with the Court using the CM/ECF system and thereby served on all counsel of record.

/s/ Amy E. Tabor
Amy E. Tabor